AMENDMENTS TO THE CLAIMS

Kindly amend claims 1 and 56 as shown in the following listing of claims. The listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims

1. (Currently Amended) A microprocessor apparatus, for performing a cryptographic operation, the apparatus comprising:

an x86-compatible microprocessor, comprising:

fetch logic, configured to fetch an application program from memory for execution by said x86-compatible microprocessor, said application program comprising:

an atomic instruction, configured to direct said x86-compatible microprocessor to perform the cryptographic operation, wherein said atomic instruction comprises:

an opcode field, configured to prescribe that said x86-compatible microprocessor accomplish the cryptographic operation as further specified within a control word stored in said memory; and

a repeat prefix field, coupled to said opcode field, configured to indicate that the cryptographic operation prescribed by the atomic instruction is to be accomplished on a plurality of blocks of input data;

a cryptography unit, configured to execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by said control word; and

an x86 integer unit, an x86 floating point unit, an x86 MMX unit, and an x86 SSE unit, wherein said cryptography unit operates in parallel with said x86 integer unit, said x86 floating point unit, said x86 MMX unit, and said x86 SSE unit, to accomplish the cryptographic operation.

~~an integer unit, coupled in parallel with said cryptography unit, configured to execute a plurality of integer operations that are required to accomplish the cryptographic operation.~~

2. (Previously Presented) The microprocessor apparatus as recited in claim 1, wherein the cryptographic operation is accomplished at the level of system privileges afforded to application programs.

3. (Previously Presented) The microprocessor apparatus as recited in claim 1, wherein the cryptographic operation comprises:

an encryption operation, said encryption operation comprising encryption of a plurality of plaintext blocks to generate a corresponding plurality of ciphertext blocks.

4. (Previously Presented) The microprocessor apparatus as recited in claim 1, wherein the cryptographic operation comprises:

a decryption operation, said decryption operation comprising decryption of a plurality of ciphertext blocks to generate a corresponding plurality of plaintext blocks.

5. (Previously Presented) The microprocessor apparatus as recited in claim 1, wherein the cryptographic operation is accomplished according to the Advanced Encryption Standard (AES) algorithm.

6. (Previously Presented) The microprocessor apparatus as recited in claim 1, wherein said atomic instruction prescribes a block cipher mode to be employed in accomplishing the cryptographic operation.

7. (Previously Presented) The microprocessor apparatus as recited in claim 6, wherein said block cipher mode comprises electronic code book (ECB) mode.

8. (Previously Presented) The microprocessor apparatus as recited in claim 6, wherein said block cipher mode comprises cipher block chaining (CBC) mode.

9. (Previously Presented) The microprocessor apparatus as recited in claim 6, wherein said block cipher mode comprises cipher feedback mode (CFB) mode.

10. (Previously Presented) The microprocessor apparatus as recited in claim 6, wherein said block cipher mode comprises output feedback (OFB) mode.

11. (Previously Presented) The microprocessor apparatus as recited in claim 1, wherein said atomic instruction prescribes that the cryptographic operation be accomplished on a plurality of text blocks.

12. (Previously Presented) The microprocessor apparatus as recited in claim 1, wherein said atomic instruction is prescribed according to the x86 instruction format.

13. (Previously Presented) The microprocessor apparatus as recited in claim 1, wherein said atomic instruction implicitly references a plurality of registers within said x86-compatible microprocessor.

14. (Previously Presented) The microprocessor apparatus as recited in claim 13, wherein said plurality of registers comprises:

a first register, wherein contents of said first register comprise a first pointer to a first memory address, said first memory address specifying a first location in said memory for access of a plurality of input text blocks upon which the cryptographic operation is to be accomplished.

15. (Previously Presented) The microprocessor apparatus as recited in claim 13, wherein said plurality of registers comprises:

a second register, wherein contents of said second register comprise a second pointer to a second memory address, said second memory address specifying a second location in said memory for storage of a corresponding plurality of output text blocks, said corresponding plurality of output text blocks being generated as a result of accomplishing the cryptographic operation upon a plurality of input text blocks.

16. (Previously Presented) The microprocessor apparatus as recited in claim 13, wherein said plurality of registers comprises:

a third register, wherein contents of said third register indicate a number of text blocks within a plurality of input text blocks.

17. (Previously Presented) The microprocessor apparatus as recited in claim 13, wherein said plurality of registers comprises:

a fourth register, wherein contents of said fourth register comprise a third pointer to a third memory address, said third memory address specifying a third location in said memory for access of cryptographic key data for use in accomplishing the cryptographic operation.

18. (Previously Presented) The microprocessor apparatus as recited in claim 17, wherein said cryptographic key data comprises a cryptographic key.

19. (Previously Presented) The microprocessor apparatus as recited in claim 17, wherein said cryptographic key data comprises a cryptographic key schedule.

20. (Previously Presented) The microprocessor apparatus as recited in claim 13, wherein said plurality of registers comprises:

a fifth register, wherein contents of said fifth register comprise a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in said memory for access of an initialization vector for use in accomplishing the cryptographic operation.

21. (Previously Presented) The microprocessor apparatus as recited in claim 13, wherein said plurality of registers comprises:

a sixth register, wherein contents of said sixth register comprise a fifth pointer to a fifth memory address, said fifth memory address specifying a fifth location in said memory for access of said control word for use in accomplishing the cryptographic operation, wherein said control word prescribes cryptographic parameters for the cryptographic operation.

22. (Previously Presented) The microprocessor apparatus as recited in claim 21, wherein said control word comprises:

an encryption/decryption field, configured to prescribe whether the cryptographic operation is an encryption operation or a decryption operation.

23. (Cancelled)

24. (Previously Presented) The microprocessor apparatus as recited in claim 1, wherein said cryptography unit comprises:

block cipher logic, configured to perform said plurality of cryptographic rounds on said each of a plurality of input text blocks according to the cryptographic operation to produce said corresponding each of a plurality of output text blocks; and

key RAM, operatively coupled to said block cipher logic, configured to store a key schedule, said key schedule comprising a plurality of round keys, each corresponding to each of said plurality of cryptographic rounds, and configured to provide said each of said plurality of round keys to said block cipher logic for performance of said each of said plurality of cryptographic rounds.

25. (Previously Presented) The microprocessor apparatus as recited in claim 1, wherein said block cipher logic is divided into two or more stages, whereby said plurality of cryptographic rounds are simultaneously performed on two or more input text blocks.

26. (Cancelled)

27. (Previously Presented) The microprocessor apparatus as recited in claim 1, wherein said opcode field directs said cryptography unit to load one of said each of said plurality of input text blocks and to perform said plurality of cryptographic rounds.

28. (Cancelled)

29. (Cancelled)

30. (Cancelled)

31. (Cancelled)

32. (Cancelled)

33. (Cancelled)

34. (Cancelled)

35. (Cancelled)

36. (Cancelled)

37. (Cancelled)

38. (Cancelled)

39. (Cancelled)

40. (Cancelled)

41. (Cancelled)

42. (Cancelled)

43. (Cancelled)

44. (Cancelled)

45. (Cancelled)

46. (Cancelled)

47. (Cancelled)

48. (Cancelled)

49. (Cancelled)

50. (Cancelled)

51. (Cancelled)

52. (Cancelled)

53. (Cancelled)

54. (Cancelled)

55. (Cancelled)

56. (Currently Amended) An apparatus for performing cryptographic operations, comprising:

an x86-compatible microprocessor, comprising:

fetch logic, configured to fetch an application program from memory for execution by said x86-compatible microprocessor, said application program comprising:

an atomic cryptographic instruction, wherein said atomic cryptographic instruction prescribes one of the cryptographic operations, said atomic cryptographic instruction comprising:

an opcode field, configured to prescribe that said microprocessor accomplish ~~the cryptographic operation~~said one of the cryptographic operations as further specified within a control word stored in said memory; and

a repeat prefix field, coupled to said opcode field, configured to indicate that ~~the cryptographic operation~~said one of the cryptographic operations prescribed by the atomic cryptographic instruction is to be accomplished on a plurality of blocks of ~~input data~~input data;

translation logic, configured to translate said atomic cryptographic instruction into associated micro instructions that specify sub-operations required to accomplish said one of the cryptographic ~~operations; and~~operations;

a cryptography unit, configured to receive a first plurality of said associated micro instructions, and configured to execute a plurality of cryptographic rounds on each of said plurality of blocks of input data to generate a corresponding each of a plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by said control word; and

an x86 integer unit, an x86 floating point unit, an x86 MMX unit, and an x86 SSE unit, wherein said cryptography unit operates in parallel with said x86 integer unit, said x86 floating point unit, said x86 MMX unit, and said x86 SSE unit, to accomplish said one of the cryptographic operations.

57. (Previously Presented) The apparatus as recited in claim 56, wherein said one of the cryptographic operations comprises:

an encryption operation, said encryption operation comprising encryption of said plurality of blocks of input data to generate a corresponding plurality of ciphertext blocks.

58. (Previously Presented) The apparatus as recited in claim 56, wherein said one of the cryptographic operations comprises:

a decryption operation, said decryption operation comprising decryption of said plurality of blocks of input data to generate a corresponding plurality of plaintext blocks.

59. (Original) The apparatus as recited in claim 56, wherein said one of the cryptographic operations is accomplished according to the Advanced Encryption Standard (AES) algorithm.

60. (Currently Amended) The apparatus as recited in claim 56, wherein said atomic cryptographic instruction prescribes a block cipher mode to be employed in accomplishing said one of the cryptographic operations.

61. (Original) The apparatus as recited in claim 60, wherein said block cipher mode comprises electronic code book (ECB) mode.

62. (Original) The apparatus as recited in claim 60, wherein said block cipher mode comprises cipher block chaining (CBC) mode.

63. (Original) The apparatus as recited in claim 60, wherein said block cipher mode comprises cipher feedback mode (CFB) mode.

64. (Original) The apparatus as recited in claim 60, wherein said block cipher mode comprises output feedback (OFB) mode.

65. (Cancelled).

66. (Currently Amended) The apparatus as recited in claim 60, wherein said atomic cryptographic instruction is prescribed according to the x86 instruction format.

67. (Currently Amended) The apparatus as recited in claim 56, wherein said atomic cryptographic instruction implicitly references a plurality of registers within said x86-compatible microprocessor.

68. (Previously Presented) The apparatus as recited in claim 67, wherein said plurality of registers comprises:

a first register, wherein contents of said first register comprise a first pointer to a first memory address, said first memory address specifying a first location in said memory for access of a said plurality of blocks of input data upon which said one of the cryptographic operations is to be accomplished.

69. (Previously Presented) The apparatus as recited in claim 67, wherein said plurality of registers comprises:

a second register, wherein contents of said second register comprise a second pointer to a second memory address, said second memory address specifying a second location in said memory for storage of a corresponding plurality of output text blocks, said corresponding plurality of output text blocks being generated as a result of accomplishing said one of the cryptographic operations upon said plurality of blocks of input data.

70. (Previously Presented) The apparatus as recited in claim 67, wherein said plurality of registers comprises:

a third register, wherein contents of said third register indicate a number of text blocks within said plurality of blocks of input data.

71. (Previously Presented) The apparatus as recited in claim 67, wherein said plurality of registers comprises:

a fourth register, wherein contents of said fourth register comprise a third pointer to a third memory address, said third memory address specifying a third location in said memory for access of cryptographic key data for use in accomplishing said one of the cryptographic operations.

72. (Original) The apparatus as recited in claim 71, wherein said cryptographic key data comprises a cryptographic key.

73. (Original) The apparatus as recited in claim 71, wherein said cryptographic key data comprises a cryptographic key schedule.

74. (Previously Presented) The apparatus as recited in claim 67, wherein said plurality of registers comprises:

a fifth register, wherein contents of said fifth register comprise a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in said memory for access of an initialization vector for use in accomplishing said one of the cryptographic operations.

75. (Previously Presented) The apparatus as recited in claim 67, wherein said plurality of registers comprises:

a sixth register, wherein contents of said sixth register comprise a fifth pointer to a fifth memory address, said fifth memory address specifying a fifth location in said memory for access of said control word for use in accomplishing said one of the cryptographic operations, wherein said control word prescribes cryptographic parameters for said one of the cryptographic operations.

76. (Original) The apparatus as recited in claim 75, wherein said control word comprises:

an encryption/decryption field, configured to prescribe whether said one of the cryptographic operations is an encryption operation or a decryption operation.

77. (Cancelled)

78. (Cancelled)

79. (Previously Presented) The apparatus as recited in claim 56, wherein said cryptography unit comprises:

block cipher logic, configured to perform said plurality of cryptographic rounds on said each of said plurality of blocks of input data according to said one of the block cryptographic operations to produce said corresponding each of a plurality of output text blocks; and

key RAM, operatively coupled to said block cipher logic, configured to store a key schedule, said key schedule comprising a plurality of round keys, each corresponding to each of said plurality of cryptographic rounds, and configured to provide said each of said plurality of round keys to said block cipher logic for performance of said each of said plurality of cryptographic rounds.

80. (Previously Presented) The apparatus as recited in claim 79, wherein said block cipher logic is divided into two or more stages, whereby said plurality of cryptographic rounds are simultaneously performed on two or more of said plurality of blocks of input data.

81. (Previously Presented) The apparatus as recited in claim 56, further comprising:

an integer unit, coupled in parallel with said cryptography unit, configured to receive a second plurality of said associated micro instructions, and configured to execute a plurality of integer operations that are required to accomplish said one of the cryptographic operations.

82. (Previously Presented) The apparatus as recited in claim 56, wherein said associated micro instructions comprise:

a first micro instruction, configured to direct said cryptography unit to load one of said each of said plurality of blocks of input data and to perform said plurality of cryptographic rounds.

83. (Original) The apparatus as recited in claim 56, wherein said one of the cryptographic operations is accomplished at the privilege level afforded to application programs.

84. (Cancelled).

85. (Cancelled).

86. (Cancelled).

87. (Cancelled).

88. (Cancelled).

89. (Cancelled).

90. (Cancelled).

91. (Cancelled).

92. (Cancelled).

93. (Cancelled).

94. (Cancelled).

95. (Cancelled).

96. (Cancelled).

97. (Cancelled).

98. (Cancelled).

99. (Cancelled).

100. (Cancelled).

101. (Cancelled).

102. (Cancelled).

103. (Cancelled).

104. (Cancelled).

105. (Cancelled).

106. (Cancelled).

107. (Cancelled).

108. (Cancelled).

109. (Cancelled).

110. (Cancelled).